PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-005641

(43)Date of publication of application : 08.01.2003

---

(51)Int.Cl. G09C 1/00
H04L 9/08
H04L 12/28

---

(21)Application number : 2001-191559 (71)Applicant : NEC CORP

(22)Date of filing : 25.06.2001 (72)Inventor : SHIMIZU MEGUMI

---

(54) METHOD AND APPARATUS FOR AUTHENTICATION IN WIRELESS LAN SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and an apparatus for authentication in a wireless LAN system which can concurrently achieve delivery of an encryption key for maintaining concealment between only parties performing wireless communication and an authenticating procedure and can simplify each authenticating procedure to the same AP (a base station) performed by a S TA (a mobile terminal) completing initial authentication after releasing the authentication.

SOLUTION: The STA searches whether a MAC address of the AP intending to perform the wireless communication exists in an AP information managing table maintained by the STA. If the MAC address does not exist in the AP information managing table, a request for authenticating a public key is transmitted to the AP. If the MAC address exists in the AP information managing table, a request for

re-authenticating the public key is transmitted to the AP.

LEGAL STATUS [Date of request for examination] 28.05.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3702812
[Date of registration] 29.07.2005
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] In the authentication approach in a wireless LAN system STA (migration terminal station) It searches whether the MAC Address of AP (base station) which is going to perform radio exists in AP information management table which said STA holds. When said MAC Address does not exist in said AP information management table Said STA performs a public key authentication demand to said AP, and said AP attests said STA, when said public key authentication demand is appropriate. When said MAC Address exists in said AP information management table It is the authentication approach in the wireless LAN system characterized by what said STA is attested for when said STA performs a public key reconfirmation certificate demand to said AP and said public key reconfirmation certificate demand is appropriate to said AP.
[Claim 2] Said AP information management table is the authentication approach in the wireless LAN system according to claim 1 characterized by holding the MAC Address of AP in which said STA gives said public key authentication demand, and the completion track record of this public key authentication has it in order of the completion track record of the newest authentication.
[Claim 3] AP private key said whose AP is its private key, and AP public key which is a public key corresponding to said AP private key, AP user certificate which is its user

certificate which attached said AP public key is held. Said STA The STA private key which is its private key, and the STA public key which is a public key corresponding to said STA private key, The authentication approach in a wireless LAN system given in any 1 term of claim 1 characterized by what the STA user certificate which is its user certificate which attached said STA public key is held for, or claim 2.

[Claim 4] The step to which said STA gives said public key authentication demand to said AP It is constituted by the public key authentication procedure. Said public key authentication procedure The step which performs an authentication demand from said STA to said AP, and the step which transmits said AP user certificate to said STA from said AP which received said authentication demand, Said STA which received said AP user certificate enciphers said STA user certificate using said AP public key attached to said AP user certificate after verifying said AP user certificate, and draws up an encryption STA user certificate. The step which transmits said encryption STA user certificate to said AP, Said AP which received said encryption STA user certificate decrypts said encryption STA user certificate with said AP private key, and reproduces said STA user certificate. Encipher the common key which said AP generated using said STA public key attached to said STA user certificate after verifying said STA user certificate, and an encryption common key is created. It consists of steps which transmit said encryption common key to said STA, and notify authentication authorization. The authentication approach in the wireless LAN system according to claim 3 characterized by what said STA which received said encryption common key decrypts said encryption common key with said STA private key, reproduces said common key, and uses this common key for subsequent frame encryption communication links for.

[Claim 5] The value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key authentication demand to said AP is the authentication approach in the wireless LAN system according to claim 4 characterized by what is been the number of the arbitration which is not "0" or "1" "n."

[Claim 6] It is the authentication approach in the wireless LAN system according to claim 5 which said AP holds a public key managed table, and is characterized by what the MAC Address of said STA in which said public key managed table has the track record that said AP notified authentication authorization in the past, said STA public key of this STA, and the common key that said AP generated at the time of authentication authorization of this STA, and published are held for in order of the newest authentication authorization.

[Claim 7] The step to which said STA gives said public key reconfirmation certificate demand to said AP It is constituted by the public key reconfirmation certificate procedure. Said public key reconfirmation certificate procedure The step which performs a reconfirmation certificate demand from said STA to said AP, and said AP

which received said reconfirmation certificate demand It searches whether the MAC Address of said STA which transmitted said public key reconfirmation certificate demand exists in said public key managed table which said AP holds. As a result of searching, the MAC Address of said STA exists in said public key managed table. and when holding said STA public key which is a public key corresponding to this MAC Address in said public key managed table is checked Said AP generates the new common key which is a new common key specified to the STA concerned. Encipher this new common key with said STA public key, and an encryption new common key is generated. It consists of steps which transmit this encryption new common key to said STA, and notify authentication authorization. The authentication approach in the wireless LAN system according to claim 6 characterized by what said STA which received said encryption new common key decrypts said encryption new common key with said STA private key, reproduces said new common key, and uses this new common key for subsequent frame encryption communication links for.

[Claim 8] The value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key reconfirmation certificate demand to said AP is the authentication approach in the wireless LAN system according to claim 7 characterized by what is been the number of the arbitration which is not "0", "1", and "n" "m."

[Claim 9] In the authentication equipment in a wireless LAN system, the MAC Address of AP (base station) which is going to perform radio searches whether it exists in AP information management table which self holds. When said MAC Address does not exist in said AP information management table When a public key authentication demand is performed to said AP and said MAC Address exists in said AP information management table Authentication equipment in the wireless LAN system characterized by having STA (migration terminal station) which performs a public key reconfirmation certificate demand to said AP, and said AP which attests said STA when said public key authentication demand from said STA or said public key reconfirmation certificate demand is appropriate.

[Claim 10] Said AP information management table is authentication equipment in the wireless LAN system according to claim 9 characterized by holding the MAC Address of AP in which said STA gives said public key authentication demand, and the completion track record of this public key authentication has it in order of the completion track record of the newest authentication.

[Claim 11] AP private key said whose AP is its private key, and AP public key which is a public key corresponding to said AP private key, AP user certificate which is its user certificate which attached said AP public key is held. Said STA The STA private key which is its private key, and the STA public key which is a public key corresponding to said STA private key, Authentication equipment in a wireless LAN system given in any 1 term of claim 9 characterized by what the STA user certificate which is its user

certificate which attached said STA public key is held for, or claim 10.

[Claim 12] When said STA performs said public key authentication demand to said AP Perform an authentication demand to said STA to said AP, and said AP user certificate is transmitted to said STA from said AP which received said authentication demand. Said STA which received said AP user certificate enciphers said STA user certificate using said AP public key attached to said AP user certificate after verifying said AP user certificate, and draws up an encryption STA user certificate. Said AP which transmitted said encryption STA user certificate to said AP, and received said encryption STA user certificate Decrypt said encryption STA user certificate with said AP private key, and said STA user certificate is reproduced. Encipher the common key which said AP generated using said STA public key attached to said STA user certificate after verifying said STA user certificate, and an encryption common key is created. Said STA which transmitted said encryption common key to said STA, notified authentication authorization, and received said encryption common key Authentication equipment in the wireless LAN system according to claim 11 characterized by what said encryption common key is decrypted with said STA private key, said common key is reproduced, and this common key is used for subsequent frame encryption communication links for.

[Claim 13] The value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key authentication demand to said AP is authentication equipment in the wireless LAN system according to claim 12 characterized by what is been the number of the arbitration which is not "0" or "1" "n."

[Claim 14] It is authentication equipment in the wireless LAN system according to claim 13 which said AP holds a public key managed table, and is characterized by what the MAC Address of said STA in which said public key managed table has the track record that said AP notified authentication authorization in the past, said STA public key of this STA, and the common key that said AP generated at the time of authentication authorization of this STA, and published are held for in order of the newest authentication authorization.

[Claim 15] When said STA performs said public key reconfirmation certificate demand to said AP Said AP which performed the reconfirmation certificate demand to said STA to said AP, and received said reconfirmation certificate demand It searches whether the MAC Address of said STA which transmitted said public key reconfirmation certificate demand exists in said public key managed table which said AP holds. As a result of searching, the MAC Address of said STA exists in said public key managed table. and when holding said STA public key which is a public key corresponding to this MAC Address in said public key managed table is checked Said AP generates the new common key which is a new common key specified to the STA concerned. Encipher this new common key with said STA public key, and an

encryption new common key is generated. Said STA which transmitted this encryption new common key to said STA, notified authentication authorization, and received said encryption new common key Authentication equipment in the wireless LAN system according to claim 14 characterized by what said encryption new common key is decrypted with said STA private key, said new common key is reproduced, and this new common key is used for subsequent frame encryption communication links for.

[Claim 16] The value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key reconfirmation certificate demand to said AP is authentication equipment in the wireless LAN system according to claim 15 characterized by what is been the number of the arbitration which is not "0", "1", and "n" "m."

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the authentication approach and authentication equipment in a wireless LAN system which enable coincidence implementation of the key delivery for codes which held secrecy nature only by between persons concerned [which performs radio], and authentication about the authentication approach and authentication equipment in a wireless LAN system in the wireless LAN system which enciphers especially data and radiocommunicates.

[0002]-

[Description of the Prior Art] In a wireless LAN (Local Area Network: run) system, in order to hold the secrecy nature of the data transmitted and received, encryption of the data frame transmitted and received is becoming indispensable conditions.

[0003] About the cipher system in a wireless LAN system, examination of a standardization is advanced until now mainly by IEEE(Institute of Electrical and Electronics Engineers : U.S., electrical-and-electric-equipment / electronic American Association of Engineers) 802 committee, and the Shared Key (common key) authentication method is adopted in IEEE802.11 which is the standard specifications as one of encryption of the wireless section in wireless LAN, and the methods of authentication.

[0004] In a Shared Key method, AP (Access Point: access point)1 as a base station of wireless LAN as shown in drawing 1 , and STA (Station : station)2 as a migration terminal office When one kind of common key which can be held for every communications partner is used or one kind of common key is not held Four kinds of common keys are held as key information common to both, and in case a frame

encryption communication link is performed, one common key in four kinds of common keys is used, choosing. However, about the delivery approach of the key for encryption, it is not defined as IEEE802.11 but has become mounting dependence.

[0005] The authentication procedure in a Shared Key method is explained with reference to drawing 10 and drawing 11 .

[0006] Drawing 10 is drawing showing the authentication procedure in a Shared Key method, and drawing 11 is drawing showing the frame body section of the frame format transmitted and received in the authentication procedure of a Shared Key method.

[0007] In drawing 10 , STA2 which performs the authentication demand by the Shared Key method to AP1 transmits the authentication frame 1 to AP1 (step S1). The frame body section of the authentication frame 1 serves as a format shown in (1) authentication frame 1 of drawing 11 , and serves as a frame which set Algorithm Number (algorithm number) 11-1-1 to "1", and set Transaction Sequence Number 11 (transaction sequence number)-1-2 to "1." In addition, at the time of the authentication in a Shared Key method, it is defined as Algorithm Number 11-1-1 to 11-4-1 being always "1."

[0008] AP1 which received the authentication demand transmits a random bit string called Challenge Text (challenge text) from STA2 to STA2 using the authentication frame 2 at step S1 (step S2). The authentication frame 2 serves as a format shown in (2) authentication frame 2 of drawing 11 , Algorithm Number 11-2-1 is "1" as above-mentioned, and Transaction Sequence Number 11-2-2 is "2", and it serves as a frame which inserted Challenge Text in Challenge Text element (challenge text element) 11-2-4.

[0009] STA2 which received the authentication frame 2 from AP1 at step S2 enciphers by one of the common keys to ICV (Integrity Check Value : integrity check value) equivalent to the CRC32 (Cyclic Redundancy Code 32bits) calculation result of Challenge Text which received from AP1, and this Challenge Text (step S3). And Challenge Text and ICV which were enciphered With IV (Initialization Vector : initialization vector) which is the key information on the used common key, it transmits to AP1 using the authentication frame 3 (step S4). The authentication frame 3 serves as a format shown in (3) authentication frame 3 of drawing 11 , Algorithm Number 11-3-1 is "1" as above-mentioned, and Transaction Sequence Number 11-3-2 is "3", and it serves as a frame which added IV 11-3-3, Challenge Text element (enciphered Challenge Text) 11-3-4, and ICV 11-3-5.

[0010] AP1 which received the authentication frame 3 by step S4 ICV which decrypted the encryption section of a receiving frame using the common key corresponding to it from the key information in a receiving frame (IV 11-3-3), and was computed from the decode result in [ICV] the receiving frame (ICV 11-3-5) Coincidence, (When coincidence with the plaintext obtained from a decode result and

Challenge Text which transmitted at step S2 is checked, and coincidence is checked at step S5), the authentication frame 4 is transmitted to STA2, and the completion of authentication is notified (step S6). The authentication frame 4 serves as a format shown in (4) authentication frame 4 of drawing 11 , Algorithm Number 11-4-1 is "1" as above-mentioned, and Transaction Sequence Number 11-4-2 is "4", and it serves as a frame which added Status Code 11 (status code)-4-9. In addition, Status Code 11-1-9, Status Code 11-2-9, Status Code 11-3-9, and Status Code 11-4-9 which were shown in drawing 11 are the information field for notifying the propriety of a frame reception success etc. to a communications partner.

[0011] By the above actuation, the authentication procedure in a Shared Key method is completed, and the frame encryption communication link using a common key is henceforth performed between STA2 and AP1.

[0012] There are technique between which third persons other than the person concerned who much various technique is proposed, for example, communicates as one of them (for example, key management server) are made to intervene, and the technique of exchanging confidential information as other one only by between persons concerned [which communicates] in the approach of authentication and key delivery in a Shared Key method. As a former example, "the authentication approach in a wireless LAN system and authentication equipment" given in JP,2001-111544,A are known, and the technique of performing encryption authentication is indicated to be an authentication server in this official report using the common key which distributed beforehand and was made to hold by a certain approach. Moreover, as a latter example, "the mutual recognition approach and its equipment" given in JP,11-191761,A are known, and the technique of checking the justification of a public key using the key delivery algorithm of Diffie-Hellman is indicated by this official report.

[0013]

[Problem(s) to be Solved by the Invention] In the system using the key management server mentioned above as the 1st example, it has the fault that the authentication procedure accompanied by encryption will become complicated, by registering the information on a migration terminal station into a key management server beforehand, and separating a key delivery procedure and an authentication procedure.

[0014] Moreover, although it becomes possible to perform key delivery which held secrecy nature only by between persons concerned [which communicates] in the authentication procedure using the key delivery algorithm mentioned above as the 2nd example, and authentication to coincidence It is what the authentication procedure becomes complicated and an operation takes much time amount. Also at the time of the authentication procedure activation for the second time at the time of the authentication discharge at the time of a communication link being cut off by the problem of a wireless propagation environment etc., the same procedure as the time

of first-time authentication will be completed, and it has the fault of increasing overhead traffic other than original data communication.

[0015] This invention is made in order to improve the situation mentioned above. The purpose of this invention While enabling coincidence implementation of the key delivery for codes, and an authentication procedure which held secrecy nature only by between persons concerned [which performs radio], it is related with STA (migration terminal station) which completed first-time authentication. It is in offering the authentication approach and authentication equipment in the wireless LAN system which makes realizable simplification of the authentication procedure of the 2nd henceforth to the same AP after authentication discharge (base station).

[0016]

[Means for Solving the Problem] The authentication approach in the wireless LAN system of this invention In the authentication approach in a wireless LAN system STA (migration terminal station) It searches whether the MAC Address of AP (base station) which is going to perform radio exists in AP information management table which said STA holds. When said MAC Address does not exist in said AP information management table Said STA performs a public key authentication demand to said AP, and said AP attests said STA, when said public key authentication demand is appropriate. When said MAC Address exists in said AP information management table, said STA performs a public key reconfirmation certificate demand to said AP, and said AP is characterized by what said STA is attested for, when said public key reconfirmation certificate demand is appropriate.

[0017] Moreover, said AP information management table is characterized by holding the MAC Address of AP which said STA performs said public key authentication demand, and has the completion track record of this public key authentication in order of the completion track record of the newest authentication.

[0018] Furthermore, AP private key said whose AP is its private key and AP public key which is a public key corresponding to said AP private key, AP user certificate which is its user certificate which attached said AP public key is held. Said STA It is characterized by what the STA private key which is its private key, the STA public key which is a public key corresponding to said STA private key, and the STA user certificate which is its user certificate which attached said STA public key are held for.

[0019] Moreover, the step to which said STA gives said public key authentication demand to said AP It is constituted by the public key authentication procedure. Said public key authentication procedure The step which performs an authentication demand from said STA to said AP, and the step which transmits said AP user certificate to said STA from said AP which received said authentication demand, Said STA which received said AP user certificate enciphers said STA user certificate using said AP public key attached to said AP user certificate after verifying said AP user certificate, and draws up an encryption STA user certificate. The step which

transmits said encryption STA user certificate to said AP, Said AP which received said encryption STA user certificate decrypts said encryption STA user certificate with said AP private key, and reproduces said STA user certificate. Encipher the common key which said AP generated using said STA public key attached to said STA user certificate after verifying said STA user certificate, and an encryption common key is created. It consists of steps which transmit said encryption common key to said STA, and notify authentication authorization. Said STA which received said encryption common key decrypts said encryption common key with said STA private key, reproduces said common key, and is characterized by what this common key is used for subsequent frame encryption communication links for.

[0020] Furthermore, the value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key authentication demand to said AP is characterized by what is been the number of the arbitration which is not "0" or "1" "n."

[0021] Moreover, said AP holds a public key managed table, and said public key managed table is characterized by what the MAC Address of said STA with the track record that said AP notified authentication authorization in the past, said STA public key of this STA, and the common key that said AP generated and published at the time of authentication authorization of this STA are held for in order of the newest authentication authorization.

[0022] Furthermore, the step to which said STA gives said public key reconfirmation certificate demand to said AP It is constituted by the public key reconfirmation certificate procedure. Said public key reconfirmation certificate procedure The step which performs a reconfirmation certificate demand from said STA to said AP, and said AP which received said reconfirmation certificate demand It searches whether the MAC Address of said STA which transmitted said public key reconfirmation certificate demand exists in said public key managed table which said AP holds. As a result of searching, the MAC Address of said STA exists in said public key managed table. and when holding said STA public key which is a public key corresponding to this MAC Address in said public key managed table is checked Said AP generates the new common key which is a new common key specified to the STA concerned. Encipher this new common key with said STA public key, and an encryption new common key is generated. It consists of steps which transmit this encryption new common key to said STA, and notify authentication authorization. Said STA which received said encryption new common key decrypts said encryption new common key with said STA private key, reproduces said new common key, and is characterized by what this new common key is used for subsequent frame encryption communication links for.

[0023] Moreover, the value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key reconfirmation certificate demand to said AP is characterized by what is been the

number of the arbitration which is not "0", "1", and "n" "m."

[0024] The authentication equipment in the wireless LAN system of this invention In the authentication equipment in a wireless LAN system, the MAC Address of AP (base station) which is going to perform radio searches whether it exists in AP information management table which self holds. When said MAC Address does not exist in said AP information management table When a public key authentication demand is performed to said AP and said MAC Address exists in said AP information management table It is characterized by having STA (migration terminal station) which performs a public key reconfirmation certificate demand to said AP, and said AP which attests said STA when said public key authentication demand from said STA or said public key reconfirmation certificate demand is appropriate.

[0025] Moreover, said AP information management table is characterized by holding the MAC Address of AP which said STA performs said public key authentication demand, and has the completion track record of this public key authentication in order of the completion track record of the newest authentication.

[0026] Furthermore, AP private key said whose AP is its private key and AP public key which is a public key corresponding to said AP private key, AP user certificate which is its user certificate which attached said AP public key is held. Said STA It is characterized by what the STA private key which is its private key, the STA public key which is a public key corresponding to said STA private key, and the STA user certificate which is its user certificate which attached said STA public key are held for.

[0027] moreover, when said STA performs said public key authentication demand to said AP Perform an authentication demand to said STA to said AP, and said AP user certificate is transmitted to said STA from said AP which received said authentication demand. Said STA which received said AP user certificate enciphers said STA user certificate using said AP public key attached to said AP user certificate after verifying said AP user certificate, and draws up an encryption STA user certificate. Said AP which transmitted said encryption STA user certificate to said AP, and received said encryption STA user certificate Decrypt said encryption STA user certificate with said AP private key, and said STA user certificate is reproduced. Encipher the common key which said AP generated using said STA public key attached to said STA user certificate after verifying said STA user certificate, and an encryption common key is created. Said encryption common key is transmitted to said STA, authentication authorization is notified, and said STA which received said encryption common key decrypts said encryption common key with said STA private key, reproduces said common key, and is characterized by what this common key is used for subsequent frame encryption communication links for.

[0028] Furthermore, the value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key authentication demand to said AP is characterized by what is been the number of the

arbitration which is not "0" or "1" "n."

[0029] Moreover, said AP holds a public key managed table, and said public key managed table is characterized by what the MAC Address of said STA with the track record that said AP notified authentication authorization in the past, said STA public key of this STA, and the common key that said AP generated and published at the time of authentication authorization of this STA are held for in order of the newest authentication authorization.

[0030] furthermore, when said STA performs said public key reconfirmation certificate demand to said AP Said AP which performed the reconfirmation certificate demand to said STA to said AP, and received said reconfirmation certificate demand It searches whether the MAC Address of said STA which transmitted said public key reconfirmation certificate demand exists in said public key managed table which said AP holds. As a result of searching, the MAC Address of said STA exists in said public key managed table. and when holding said STA public key which is a public key corresponding to this MAC Address in said public key managed table is checked Said AP generates the new common key which is a new common key specified to the STA concerned. Encipher this new common key with said STA public key, and an encryption new common key is generated. This encryption new common key is transmitted to said STA, authentication authorization is notified, and said STA which received said encryption new common key decrypts said encryption new common key with said STA private key, reproduces said new common key, and is characterized by what this new common key is used for subsequent frame encryption communication links for.

[0031] Moreover, the value of Algorithm Number of the frame body section in the MAC frame transmitted and received in case said STA performs said public key reconfirmation certificate demand to said AP is characterized by what is been the number of the arbitration which is not "0", "1", and "n" "m."

[0032]

[Embodiment of the Invention] Next, the gestalt of operation of this invention is explained with reference to a drawing.

[0033] Drawing 1 is the block diagram showing 1 operation gestalt of the authentication equipment in the wireless LAN system of this invention.

[0034] The gestalt of this operation shown in drawing 1 consists of two or more STA (Station : station)2 (STA [2-1], STA2-k) as a migration terminal office which belongs to AP (Access Point: access point)1 and AP1 as a base station of wireless LAN. The gestalt of operation shown in drawing 1 is an Infrastructure (infrastructure) method which IEEE802.11 defines, and says the smallest unit of such a wireless LAN network as BSS (Basic Service Set : basic service set)4.

[0035] AP1 in BSS4 the Beacon (beacon) frame including information for each STA2 to synchronize with AP1 Each STA2 in BSS4 which carried out broadcasting

transmission into BSS4 periodically, and received the Beacon frame concerned After performing an authentication demand to AP1 at the time of communication link initiation and obtaining authentication authorization by AP1, it becomes possible by completing the imputed processing to AP1 to perform the communication link with AP1. Moreover, each STA2 in BSS4 in an Infrastructure method performs the communication link which minded AP1 at the time of the communication link between STAs2.

[0036] Moreover, although AP1 in drawing 1 serves as (portal), Portal shows that the protocol conversion function with LAN protocols other than IEEE802.11 was added to AP1, and shows that it is the base station which enabled connection with the cables LAN as a base station, such as AP1 and Ethernet (trademark) (Ethernet (trademark))5.

[0037] In addition, although the gestalt of operation shown in drawing 1 is based on IEEE802.11, unlike a Shared Key method (common key authentication method), in the gestalt of this operation, the authentication method using a private key and a public key is mainly used for it as encryption of the wireless section, and a method of authentication. Therefore, in order to distinguish from a Shared Key method, suppose that the authentication method in this operation gestalt is called a public key authentication method for convenience.

[0038] Next, with reference to drawing 2 , the detail configuration of AP1 and STA2 is explained.

[0039] Drawing 2 is the detail block diagram showing an example of AP and STA.

[0040] In drawing 2 , the block diagram of an upper case is AP1, and the block diagram of the lower berth is STA2.

[0041] AP1 minds the high order layer interface 17-1 which is an interface of the wireless LAN card 19-1 shown in drawing 2 , and a high order layer. Higher-level protocol processing of TCP/IP (Transport Control Protocol/Internet Protocol), various applications, etc. It is what is realized by the base station terminal body 18. STA2 The migration terminal bodies 20, such as a note type personal computer, realize the same higher-level protocol processing as AP1 through the high order layer interface 17-2 which is an interface of the wireless LAN card 19-2 shown in drawing 2 , and a high order layer.

[0042] The wireless LAN card 19-1 and the wireless LAN card 19-2 which are shown in drawing 2 are equipped with the same configuration. Therefore, in the wireless LAN card 19, the thing corresponding to the same component shall attach the same reference figure or the same sign.

[0043] The wireless LAN card 19 (19-1 and 19-2) shown in drawing 2 The walkie-talkie section 12 which performs frame transmission and reception in the wireless section, and the IEEE802.11 PHY (Physical Layer: physical layer) protocol processing section 13 which performs strange recovery processing, The IEEE802.11 MAC protocol processing section 14 which performs the access control in a MAC

(Medium Access Control : media access control) layer, It consists of a CPU which builds in high order layer processing of authentication processing in a MAC layer etc., the high order layer processing section 15 realized by memory 16, and memory 16 which the high order layer processing section 15 uses.

[0044] Next, in case STA2 requires authentication from AP1 with reference to drawing 3 , the MAC frame transmitted and received between STA2 and AP1 is explained.

[0045] Drawing 3 is drawing explaining the configuration of the MAC frame transmitted and received by the authentication demand between AP and STA.

[0046] It is exchanged between AP1 and STA2 by the authentication demand to AP1 of STA2 in the MAC frame 30-1 according to the MAC frame format of IEEE802.11 shown in drawing 3 , and the MAC frame 30-1 is constituted from MAC Header (MAC header) 30-2, and FrameBody 30 (frame body)-3 and FCS30(Frame Check Sequence: frame check sequence)-4.

[0047] And MAC Header 30-2 in an Infrastructure method The field of Frame Control 30 (frame control)-11 which shows various frame types and control information, The field of Duration (DEYURESHON) 30-12 which defines the time amount for performing transmitting standby when a transmission place is busy, The field of DA (Destination Address : transmission place address) 30-13 which shows the frame transmission place address, The field of SA (Source Address: transmitting agency address) 30-14 which shows the transmitting agency address of a frame, It consists of the field of BSSID 30-15 which shows the identification information of BSS4, and the field of Sequence Control (sequential control) 30-16 which shows the order of frame transmission.

[0048] In the IEEE802.11 MAC protocol processing section 14 shown in drawing 2 , at the time of frame transmission Put the Request-to-Send frame from the high order layer processing section 15 into FrameBody 30-3 shown in drawing 3 , and it is encapsulated. MAC Header 30-2 created from Request-to-Send information is added before FrameBody 30-3. The CRC32 (Cyclic Redundancy Code 32bits) calculation result of MAC Header 30-2 and FrameBody 30-3 concerned By adding behind FrameBody 30-3 as FCS 30-4, conversion on the MAC frame 30-1 according to an IEEE802.11 MAC protocol as shown in drawing 3 is performed. Then, in the IEEE802.11 PHY protocol processing section 13 shown in drawing 2 , transmitting processing is completed by performing modulation processing to the MAC frame 30-1 concerned, and sending out the MAC frame 30-1 concerned on space through the walkie-talkie section 12.

[0049] In the IEEE802.11 MAC protocol processing section 14 shown in drawing 2 , at the time of frame reception It is CRC32 to the MAC frame 30-1 received as a result of having performed recovery processing in the IEEE802.11 PHY protocol processing section 13 through the walkie-talkie section 12. It calculates. The value and CRC32 of

FCS 30-4 in a receiving frame When a calculation result is in agreement, processing to the analysis and the receiving frame of the contents of MAC Header 30-2 is performed, and the part of FrameBody 30-3 is notified to the high order layer processing section 15.

[0050] Next, with reference to drawing 4 and drawing 5 , the public key managed table and AP information management table as an important component of this operation gestalt are explained.

[0051] Drawing 4 is drawing explaining the public key managed table which AP holds, and drawing 5 is drawing explaining AP information management table which STA holds.

[0052] AP1 is held in the memory 16 of the wireless LAN card 19-1 which shows the public key managed table 40 shown in drawing 4 to drawing 2 . The column of STA Mac Address 40 (MAC Address of STA)-1 holding the MAC Address which is a physical address of the MAC layer of STA2 with which the public key managed table 40 has the track record that AP1 performed authentication authorization in public key authentication of this invention in the past, It consists of a column of Public Key (public key) 40-2 holding the public key of STA2 concerned, and a column of Shared Key (shared key) 40-3 holding the common key which AP1 published to STA2 concerned at the time of authentication authorization. And AP1 registers each line of the public key managed table 40 in order of the newest authentication authorization of STA2.

[0053] STA2 is held in the memory 16 of the wireless LAN card 19-2 which shows AP information management table 50 shown in drawing 5 to drawing 2 . AP information management table 50 consists of columns of AP MAC Address (MAC Address of AP) 50-1 to which STA2 holds the MAC Address of AP1 which requires public key authentication of this invention and has the completion track record of this public key authentication, and STA2 registers each line of AP information management table 50 in order of the completion track record of the newest authentication of AP1.

[0054] At the time of the information registration to the public key managed table 40 explained by drawing 4 , AP1 moves the information concerned to the line of the head of the public key managed table 40 with the renewal of information of the contents of registration, when registered STA MAC address 40-1 is searched and the same registered MAC Address already exists. For every [moreover,] implementation of the frame encryption communication link after the completion of public key authentication of this invention By AP's1 searching STA MAC address 40-1 of the public key managed table 40, and moving the management information of STA2 of a communications partner to the line of the head of the public key managed table 40 When the public key managed table 40 reaches a marginal number of registration and it becomes impossible by positioning the management information of a communications partner with a new transmitter meeting in a managed table high order

to new information register it It corresponds by deleting the management information of the oldest communications partner of the transmitter meeting most located in low order within the public key managed table 40.

[0055] Moreover, like AP1, at the time of the information registration to AP information management table 50 explained by drawing 5 , STA2 moves the information concerned to the line of the head of AP information management table 50 with the renewal of information of the contents of registration, when registered AP MAC address 50-1 is searched and the same registered MAC Address already exists. For every [moreover,] implementation of the frame encryption communication link after the completion of public key authentication of this invention By STA's2 searching AP MAC address 50-1 of AP information management table 50, and moving the management information of AP1 of a communications partner to the line of the head of AP information management table 50 When AP information management table 50 reaches a marginal number of registration and it becomes impossible by positioning the management information of a communications partner with a new transmitter meeting in a managed table high order to new information register it It corresponds by deleting the management information of the oldest communications partner of the transmitter meeting most located in low order within AP information management table 50.

[0056] Next, actuation of this operation gestalt is explained with reference to drawing 6 , drawing 7 , drawing 8 , and drawing 9 .

[0057] In this operation gestalt, both AP1 which is the base station of the wireless LAN system shown in drawing 1 , and STA2 which is a migration terminal office shall hold the user certificate which attached its private key, public key corresponding to it, and this public key. And the user certificate concerned shall be premised on the conditions that the relation between a public key and its carrier (namely, AP1 or STA2) and own justification of a carrier can be proved, by the third person represented by the certificate authority. Below, a user certificate shall mean a digital user certificate.

[0058] When STA2 in drawing 1 tends to perform radio through AP1, STA2 is first started from transmitting the public key authentication demand of this invention to AP1.

[0059] STA2 searches AP MAC Address 50-1 in AP information management table 50 which used the MAC Address of AP1 of an authentication demand place at the time of public key authentication initiation, and was shown in drawing 5 at it. When the MAC Address of the authentication demand place AP 1 does not exist in AP information management table 50 When the public key authentication procedure shown in drawing 6 as a first-time authentication demand is performed and the MAC Address of the authentication demand place AP 1 exists, since it is the case with AP1 concerned where there is a completion track record of public key authentication, the public key

reconfirmation certificate procedure shown in drawing 8 is performed as a reconfirmation certificate in the past.

[0060] First, the public key authentication procedure as a first-time authentication demand is explained with reference to drawing 6 and drawing 7 .

[0061] Drawing 6 is drawing showing a public key authentication procedure, and drawing 7 is drawing showing the frame body section (FrameBody 30-3 of drawing 3) of the MAC frame transmitted and received in a public key authentication procedure.

[0062] In drawing 6 , STA2 which performs the authentication demand by the public key authentication procedure to AP1 transmits the authentication frame 61 to AP1 (step S61). The frame body section of the authentication frame 61 serves as a format shown in (1) authentication frame 61 of drawing 7 , and serves as a frame which set Algorithm Number (algorithm number) 70-1-1 to "n", and set Transaction Sequence Number 70 (transaction sequence number)-1-2 to "1." In addition, at the time of the authentication in a public key authentication procedure, Algorithm Number 70-1-1 to 70-4-1 always defines it as what is "n" (the number of the arbitration whose n is not "0" or "1"). By setting Algorithm Number 70-1-1 to 70-4-1 to "n", it becomes possible to distinguish from the authentication procedure by the Shared Key method.

[0063] AP1 which received the public key authentication demand transmits the user certificate which AP1 holds using the authentication frame 62 from STA2 to STA2 at step S61 (step S62). The authentication frame 62 serves as a format shown in (2) authentication frame 62 of drawing 7 , Algorithm Number 70-2-1 is "n" as above-mentioned, and Transaction Sequence Number 70-2-2 is "2", and it serves as a frame which inserted the user certificate (what also attached the public key of AP1 which accompanies a user certificate) which AP1 holds in the user certificate 70-2-3 of AP.

[0064] STA2 which received the authentication frame 62 from AP1 at step S62 verifies the contents of the user certificate of AP1 which received from AP1, and if it checks that there is no problem in the verification result of the user certificate of AP1, the user certificate which STA2 holds will be enciphered using the public key attached to the user certificate of AP1 (step S63). And the user certificate of enciphered STA2 is transmitted to AP1 with the public key of STA2 which accompanies the user certificate of STA2 using the authentication frame 63 (step S64). The authentication frame 63 is STA which had become the format shown in (3) authentication frame 63 of drawing 7 , and Algorithm Number 70-3-1 is "n" as above-mentioned, and Transaction Sequence Number 70-3-2 is "3", and was enciphered with the public key of AP. It is the frame which added the user certificate 70-3-3.

[0065] AP1 which received the authentication frame 63 at step S64 STA enciphered with the public key of AP The user certificate 70-3-3 is decrypted with the private key of AP1. The contents of the user certificate of STA2 are verified, and if it checks that there is no problem in the verification result of the user certificate of STA2, the

common key which generated the common key next this time and was generated using the public key attached to the user certificate of STA2 will be enciphered (step S65). And the enciphered common key is transmitted to STA2 using the authentication frame 64, and authentication authorization is notified (step S66). It is the format shown in (4) authentication frame 64 of drawing 7 , and Algorithm Number 70-4-1 is "n" as above-mentioned, Transaction Sequence Number 70-4-2 is "4", and the authentication frame 64 is STA. It is the frame which added the common key 70-4-3 enciphered with the public key. In addition, Status Code 70-1-9, Status Code 70-2-9, Status Code 70-3-9, and Status Code 70-4-9 which were shown in drawing 7 are the information field for notifying the propriety of a frame reception success etc. to a communications partner.

[0066] Then, STA2 which received the authentication frame 64 from AP1 at step S66 is STA. The common key 70-4-3 enciphered with the public key will be decrypted with the private key of STA2, the common key which AP1 generated will be restored, and this common key will be used for the frame encryption in the radio actually performed after this (step S67). By the above actuation, a public key authentication procedure is ended and a frame encryption communication link will be henceforth performed between STA2 and AP1.

[0067] Next, the public key reconfirmation certificate procedure at the time of a reconfirmation certificate being performed is explained with reference to drawing 8 and drawing 9 .

[0068] Drawing 8 is drawing showing a public key reconfirmation certificate procedure, and drawing 9 is drawing showing the frame body section (FrameBody 30-3 of drawing 3) of the MAC frame transmitted and received in a public key reconfirmation certificate procedure.

[0069] In drawing 8 , STA2 which had the completion track record of public key authentication in the past to AP1 of an authentication demand place transmits the authentication frame 81 to AP1 as a public key reconfirmation certificate demand (step S81). The frame body section of the authentication frame 81 serves as a format shown in (1) authentication frame 81 of drawing 9 , and serves as a frame which set Algorithm Number (algorithm number) 90-1-1 to "m", and set Transaction Sequence Number 90 (transaction sequence number)-1-2 to "1." In addition, at the time of the authentication in a public key reconfirmation certificate procedure, Algorithm Number 90-1-1 to 90-2-1 always defines it as what is "m" (the number of the arbitration whose m is not "0", "1", and "n"). By setting Algorithm Number 90-1-1 to 90-2-1 to "m", it becomes possible to distinguish from the public key authentication procedure shown in drawing 6 .

[0070] In the public key managed table 40 shown in drawing 4 which AP1 holds, the MAC Address of STA2 which transmitted the public key reconfirmation certificate demand exists in STA Mac Address 40-1, or AP1 which received the public key

reconfirmation certificate demand from STA2 at step S81 searches (step S82). And when retrieval being successful and holding the public key corresponding to it in the column of Public Key 40-2 is checked, AP1 newly generates the common key specified to STA2 concerned, and enciphers it using the public key (public key of STA2 concerned) which acquired this new common key from Public Key 40-2 of the public key managed table 40 (step S83). And the enciphered new common key is transmitted to STA2 using the authentication frame 82 (step S84). It is the format shown in (2) authentication frame 82 of drawing 9 , and Algorithm Number 90-2-1 is "m" as above-mentioned, Transaction Sequence Number 90-2-2 is "2", and the authentication frame 82 is STA. It is the frame which added the new common key 90-2-3 enciphered with the public key. In addition, Status Code 90-1-9 and Status Code 90-2-9 which were shown in drawing 9 are the information field for notifying the propriety of a frame reception success etc. to a communications partner.

[0071] Then, STA2 which received the authentication frame 82 from AP1 at step S84 is STA. It will decrypt with the private key with which STA2 holds the new common key 90-2-3 enciphered with the public key, the new common key which AP1 newly generated will be restored, and this new common key will be used for the frame encryption in the radio actually performed after this (step S85). By the above actuation, a public key reconfirmation certificate procedure is ended, and a frame encryption communication link will be henceforth performed between STA2 and AP1.

[0072] In the above, the 1st operation gestalt of this invention was explained to the detail. The public key corresponding to [in / both / the 1st operation gestalt] one's private key and it in AP1 and STA2, And the user certificate which attached the public key is held and the user certificate concerned is the basis of the conditions [third person-/ who is represented by the certificate authority] that the relation between a public key and its carrier and own justification of a carrier can be proved. Although the exchange procedure of the public key shown in drawing 6 will occur by the time STA2 performs a public key authentication demand to AP1 and obtains authentication authorization from AP1 Based on this invention, a partner's public key information that the completion track record of authentication has AP1 and STA2, by continuing holding after authentication discharge By using the public key reconfirmation certificate procedure shown in drawing 8 in the authentication demand of the 2nd henceforth, it has the effectiveness that simplification of authentication procedure is attained, by skipping the public key exchange procedure between AP1 and STAs2 which were performed in the first-time authentication procedure.

[0073] Moreover, by using a user certificate in the public key authentication procedure of the first time shown in drawing 6 From holding the public key information on STA2 after the authentication authorization after checking the public key of STA2, and the justification of STA2 which is the carrier, AP1 When the reconfirmation certificate demand which used the MAC Address of STA2 concerned and which is

depended for becoming completely occurs AP1 which performs the public key reconfirmation certificate procedure shown in drawing 8 In order to encipher with the public key corresponding to the private key with which only just STA2 holds the common key transmitted to STA2, It has the effectiveness of becoming possible for the reconfirmation certificate demand origin STA depended for becoming completely to be unable to decrypt this, and to be unable to acquire a common key, therefore to prevent ********** by inaccurate STA by this invention.

[0074] Next, the 2nd operation gestalt of this invention is explained.

[0075] the 2nd operation gestalt be the wireless LAN system considered a system as the configuration which make public key management information (public key managed table 40 specifically showed in drawing 4) about STA under attribution in each AP (migration terminal office) the share information in a combination network in the combination network top where two or more BSS (basic service set) by two or more AP (base station) exist , and each BSS be connect by the cable or wireless . The configuration made into the share information in a combination network is a configuration of arranging the high order AP which generalizes two or more AP, the high order AP holding public key management information collectively, and each AP performing the registration or the inquiry to a high order AP at the time of the need, and obtaining the reply from a high order AP. Also in case STA under attribution in Arbitration AP performs first-time public key authentication to other AP by migration of BSS by considering as such a configuration, it has the effectiveness that simplification of authentication procedure is attained, by carrying out the public key reconfirmation certificate procedure by this invention.

[0076] Next, the 3rd operation gestalt of this invention is explained.

[0077] The 3rd operation gestalt is Independent which IEEE802.11 defines. It is the configuration which applies this invention of the 1st operation gestalt to the wireless LAN system of a method (independent: independence). Independent By the method, only two or more STAs exist in IBSS (Independent BSS : independent BSS), and AP does not exist. And STA which received the public key authentication demand based on the 1st operation gestalt of this invention at the time of the public key authentication between STAs in IBSS considers as the configuration which continues holding the public key management information (public key managed table 40 specifically shown in drawing 4) of the authentication demand origin STA. By considering as such a configuration, it has the effectiveness that simplification of the public key reconfirmation certificate procedure of the 2nd henceforth is attained.

[0078] In addition, in the 1st [of this invention], 2nd, and 3rd operation gestalten, it becomes possible to prevent continuation use of an expiration date piece user certificate by considering as the configuration which gives the maintenance term of public key management information by introducing the expiration date information based on a user certificate with the public key management information about the

authentication demand origin STA which the inside [STA] AP of BSS which performs authentication authorization, and IBSS holds.

[0079]

[Effect of the Invention] As explained above, the authentication approach and authentication equipment in a wireless LAN system of this invention Since coincidence implementation of the key delivery for codes and an authentication procedure which held secrecy nature only by between persons concerned [which performs radio] can be enabled, it is related with STA (migration terminal office) which completed first-time authentication. It has the effectiveness of making realizable simplification of the authentication procedure of the 2nd henceforth to the same AP after authentication discharge (base station).

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing 1 operation gestalt of the authentication equipment in the wireless LAN system of this invention.

[Drawing 2] It is the detail block diagram showing an example of AP and STA.

[Drawing 3] It is drawing explaining the configuration of the MAC frame transmitted and received by the authentication demand between AP and STA.

[Drawing 4] It is drawing explaining the public key managed table which AP holds.

[Drawing 5] It is drawing explaining AP information management table which STA holds.

[Drawing 6] It is drawing showing a public key authentication procedure.

[Drawing 7] It is drawing showing the frame body section of the MAC frame transmitted and received in a public key authentication procedure.

[Drawing 8] It is drawing showing a public key reconfirmation certificate procedure.

[Drawing 9] It is drawing showing the frame body section of the MAC frame transmitted and received in a public key reconfirmation certificate procedure.

[Drawing 10] It is drawing showing the authentication procedure in a Shared Key method.

[Drawing 11] It is drawing showing the frame body section of the frame format transmitted and received in the authentication procedure of a Shared Key method.

[Description of Notations]

1 AP

2 STA

4 BSS

5 Ethernet (Ethernet)

12 Walkie-talkie Section
13 IEEE802.11 PHY Protocol Processing Section
14 IEEE802.11 MAC Protocol Processing Section
15 High Order Layer Processing Section
16 Memory
17 High Order Layer Interface
18 Base Station Terminal Body
19 Wireless LAN Card
20 Migration Terminal Body

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－5641
（P2003－5641A）
(43)公開日　平成15年１月８日(2003.1.8)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｚ　５Ｊ１０４
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	12/28	３００Ｚ　５Ｋ０３３
	12/28	３００		9/00	６０１Ｃ
					６０１Ｅ

審査請求　有　　請求項の数16　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－191559(P2001－191559)

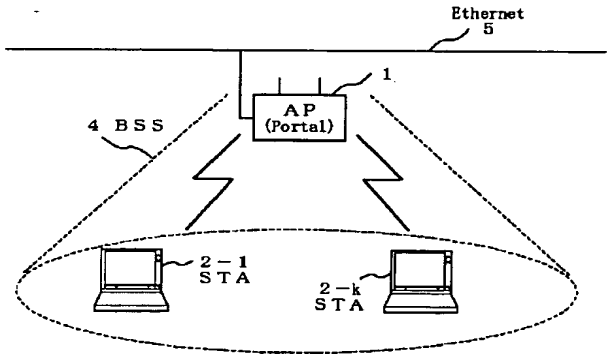
(22)出願日　平成13年６月25日(2001.6.25)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　清水　めぐみ
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100082935
弁理士　京本　直樹　（外２名）

Ｆターム(参考)　5J104 AA07 AA16 EA06 EA19 KA02
KA05 KA06 NA02 NA20
5K033 AA08 CC02 DA01 DA19

(54)【発明の名称】　無線ＬＡＮシステムにおける認証方法と認証装置

(57)【要約】
【課題】無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配送と認証手順の同時実現を可能とすると共に、初回の認証を完了したＳＴＡ（移動端末局）に関しては、認証解除後の同一ＡＰ（基地局）に対する２回目以降の認証手順の簡略化を実現可能とする、無線ＬＡＮシステムにおける認証方法と認証装置を提供する。
【解決手段】ＳＴＡは、無線通信を行おうとするＡＰのＭＡＣアドレスがＳＴＡの保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＡＰに対して公開鍵認証要求を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＡＰに対して公開鍵再認証要求を行うことを特徴とする。



1

【特許請求の範囲】

【請求項１】　無線ＬＡＮシステムにおける認証方法において、ＳＴＡ（移動端末局）は、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが前記ＳＴＡの保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＳＴＡは前記ＡＰに対して公開鍵認証要求を行い、前記ＡＰは前記公開鍵認証要求が妥当である場合には前記ＳＴＡの認証を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＳＴＡは前記ＡＰに対して公開鍵再認証要求を行い、前記ＡＰは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う、ことを特徴とする無線ＬＡＮシステムにおける認証方法。

【請求項２】　前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする請求項１に記載の無線ＬＡＮシステムにおける認証方法。

【請求項３】　前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする請求項１或いは請求項２の何れか１項に記載の無線ＬＡＮシステムにおける認証方法。

【請求項４】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行うステップは、公開鍵認証手順によって構成され、前記公開鍵認証手順は、前記ＳＴＡから前記ＡＰに対して認証要求を行うステップと、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信するステップと、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信するステップと、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に

2

該共通鍵を使用する、ことを特徴とする請求項３に記載の無線ＬＡＮシステムにおける認証方法。

【請求項５】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを特徴とする請求項４に記載の無線ＬＡＮシステムにおける認証方法。

【請求項６】　前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする請求項５に記載の無線ＬＡＮシステムにおける認証方法。

【請求項７】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行うステップは、公開鍵再認証手順によって構成され、前記公開鍵再認証手順は、前記ＳＴＡから前記ＡＰに対して再認証要求を行うステップと、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする請求項６に記載の無線ＬＡＮシステムにおける認証方法。

【請求項８】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、ことを特徴とする請求項７に記載の無線ＬＡＮシステムにおける認証方法。

【請求項９】　無線ＬＡＮシステムにおける認証装置において、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが自身の保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＡＰに対して公開鍵認証要求を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＡＰに対して公開鍵再認証要求を行うＳＴＡ（移動端末

局）と、前記ＳＴＡからの前記公開鍵認証要求あるいは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う前記ＡＰと、を備えることを特徴とする無線ＬＡＮシステムにおける認証装置。

【請求項１０】　前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする請求項９に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１１】　前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする請求項９或いは請求項１０の何れか１項に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１２】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して認証要求を行い、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信し、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信し、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする請求項１１に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１３】　前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを特徴とする請求項１２に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１４】　前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする請求項１３に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１５】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して再認証要求を行い、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする請求項１４に記載の無線ＬＡＮシステムにおける認証装置。

【請求項１６】　前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、ことを特徴とする請求項１５に記載の無線ＬＡＮシステムにおける認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は無線ＬＡＮシステムにおける認証方法と認証装置に関し、特にデータを暗号化して無線通信する無線ＬＡＮシステムにおいて、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配送と認証の同時実現を可能とする、無線ＬＡＮシステムにおける認証方法と認証装置に関する。

【０００２】

【従来の技術】無線ＬＡＮ（Local Area Network：ラン）システムにおいては、送受信するデータの秘匿性を保持するために、送受信するデータフレームの暗号化が必須の条件となってきている。

【０００３】無線ＬＡＮシステムにおける暗号化方式については、これまでＩＥＥＥ（Institute of Electrical and Electronics Engineers ：米国、電気／電子技術者協会）８０２委員会を中心として標準化の検討が進められてきており、その標準仕様であるIEEE802.11においては、無線ＬＡＮにおける無線区間の暗号化及び認証の方式の１つとして、Shared Key（共通鍵）認証方式が採用されている。

【０００４】Shared Key方式においては、図１に示すよ

5

うな無線ＬＡＮの基地局としてのＡＰ（Access Point：アクセスポイント）１と移動端末局としてのＳＴＡ（Station ：ステーション）２とが、通信相手毎に互いに保持することのできる１種類の共通鍵を使用する、又は１種類の共通鍵を保持していない場合には、両者共通の鍵情報として４種類の共通鍵を保持しておき、フレーム暗号化通信を行う際には４種類の共通鍵の中の１つの共通鍵を選択して使用するようになっている。しかし、暗号化用の鍵の配送方法に関しては、IEEE802.11には定義されておらず、実装依存となっている。

【０００５】Shared Key方式における認証手順について、図１０及び図１１を参照して説明する。

【０００６】図１０は、Shared Key方式における認証手順を示す図であり、図１１は、Shared Key方式の認証手順において送受信されるフレームフォーマットのフレームボディ部を示す図である。

【０００７】図１０において、ＡＰ１に対してShared Key方式による認証要求を行うＳＴＡ２は、ＡＰ１に対して認証フレーム１を送信する（ステップＳ１）。認証フレーム１のフレームボディ部は、図１１の（１）認証フレーム１に示す形式となっており、Algorithm Number（アルゴリズム番号）１１－１－１を「１」とし、Transaction Sequence Number （トランザクションシーケンス番号）１１－１－２を「１」としたフレームとなっている。なお、Shared Key方式における認証時には、Algorithm Number１１－１－１～１１－４－１は常に「１」であると定義されている。

【０００８】ステップＳ１でＳＴＡ２から認証要求を受信したＡＰ１は、認証フレーム２を用いてChallenge Text（チャレンジテキスト）というランダムなビット列をＳＴＡ２に対して送信する（ステップＳ２）。認証フレーム２は、図１１の（２）認証フレーム２に示す形式となっており、Algorithm Number１１－２－１は前述の通り「１」であり、Transaction Sequence Number １１－２－２は「２」で、Challenge Text element（チャレンジテキストエレメント）１１－２－４にChallenge Textを挿入したフレームとなっている。

【０００９】ステップＳ２でＡＰ１から認証フレーム２を受信したＳＴＡ２は、ＡＰ１から受信したChallenge Textと、該Challenge Textに対するCRC32(Cyclic Redundancy Code 32bits)算出結果に相当するICV （Integrity Check Value ：インテグリティチェックバリュー）に対して、共通鍵の１つで暗号化を行う（ステップＳ３）。そして、暗号化したChallenge TextとICV を、使用した共通鍵の鍵情報であるIV（Initialization Vector ：イニシャライゼイション・ベクター）と共に、認証フレーム３を用いてＡＰ１に対して送信する（ステップＳ４）。認証フレーム３は、図１１の（３）認証フレーム３に示す形式となっており、Algorithm Number１１－３－１は前述の通り「１」であり、Transaction Sequence Number １１－３－２は「３」で、IV１１－３－３、Challenge Text element（暗号化したChallenge Text）１１－３－４、ICV １１－３－５を付加したフレームとなっている。

6

【００１０】ステップＳ４で認証フレーム３を受信したＡＰ１は、受信フレーム内鍵情報（IV１１－３－３）からそれに対応する共通鍵を用いて受信フレームの暗号化部を復号化し、受信フレーム内ICV （ICV １１－３－５）と復号結果から算出したICV の一致と、復号結果から得られる平文とステップＳ２で送信したChallenge Textとの一致を確認した場合には（ステップＳ５で一致を確認した場合）、認証フレーム４をＳＴＡ２に対して送信して認証完了を通知する（ステップＳ６）。認証フレーム４は、図１１の（４）認証フレーム４に示す形式となっており、Algorithm Number１１－４－１は前述の通り「１」であり、Transaction Sequence Number １１－４－２は「４」で、Status Code （ステータスコード）１１－４－９を付加したフレームとなっている。なお、図１１に示したStatus Code １１－１－９、Status Code １１－２－９、Status Code １１－３－９及びStatus Code １１－４－９は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【００１１】以上の動作により、Shared Key方式における認証手順が終了し、以後、ＳＴＡ２とＡＰ１間で共通鍵を用いたフレーム暗号化通信が行われるようになっている。

【００１２】Shared Key方式における認証と鍵配送の方法には、様々な手法が多数提案されており、例えばその１つとして、通信を行う当事者以外の第三者（例えば鍵管理サーバ）を介在させる手法や、他の１つとして、通信を行う当事者間でのみ秘密情報の交換を行う手法がある。前者の一例としては、特開２００１－１１１５４４号公報記載の「無線ＬＡＮシステムにおける認証方法と認証装置」が知られており、この公報では、認証サーバと、何らかの方法で予め配布し保持させた共通鍵を用いて、暗号化認証を行う技術が記載されている。また、後者の一例としては、特開平１１－１９１７６１号公報記載の「相互認証方法及びその装置」が知られており、この公報では、Diffie-Hellmanの鍵配送アルゴリズムを用いて公開鍵の正当性を確認する技術が記載されている。

【００１３】

【発明が解決しようとする課題】第１の例として上述した鍵管理サーバを利用したシステムでは、予め移動端末局の情報を鍵管理サーバに登録しておくものであり、鍵配送手順と認証手順が分離されることにより、暗号化を伴う認証手順が複雑なものとなるという欠点を有している。

【００１４】また、第２の例として上述した鍵配送アルゴリズムを用いた認証手順においては、通信を行う当事者間でのみ秘匿性を保持した鍵配送と認証を同時に行う

ことが可能となるが、その認証手順が複雑となり演算に多くの時間を要するものとなっており、無線伝播環境の問題などによって通信が絶たれた際の認証解除時における再度の認証手順実行時にも、初回の認証時と同一手順を踏むこととなり、本来のデータ通信以外のオーバーヘッドトラヒックを増大させてしまうという欠点を有している。

【００１５】本発明は上述した事情を改善するためになされたものであり、本発明の目的は、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配送と認証手順の同時実現を可能とすると共に、初回の認証を完了したＳＴＡ（移動端末局）に関しては、認証解除後の同一ＡＰ（基地局）に対する２回目以降の認証手順の簡略化を実現可能とする、無線ＬＡＮシステムにおける認証方法と認証装置を提供することにある。

【００１６】

【課題を解決するための手段】本発明の無線ＬＡＮシステムにおける認証方法は、無線ＬＡＮシステムにおける認証方法において、ＳＴＡ（移動端末局）は、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが前記ＳＴＡの保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＳＴＡは前記ＡＰに対して公開鍵認証要求を行い、前記ＡＰは前記公開鍵認証要求が妥当である場合には前記ＳＴＡの認証を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＳＴＡは前記ＡＰに対して公開鍵再認証要求を行い、前記ＡＰは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う、ことを特徴とする。

【００１７】また、前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする。

【００１８】さらに、前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする。

【００１９】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行うステップは、公開鍵認証手順によって構成され、前記公開鍵認証手順は、前記ＳＴＡから前記ＡＰに対して認証要求を行うステップと、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信するステップと、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書

を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信するステップと、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする。

【００２０】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを特徴とする。

【００２１】また、前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする。

【００２２】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行うステップは、公開鍵再認証手順によって構成され、前記公開鍵再認証手順は、前記ＳＴＡから前記ＡＰに対して再認証要求を行うステップと、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知するステップとから構成され、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする。

【００２３】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、

ことを特徴とする。

【００２４】本発明の無線ＬＡＮシステムにおける認証装置は、無線ＬＡＮシステムにおける認証装置において、無線通信を行おうとするＡＰ（基地局）のＭＡＣアドレスが自身の保持するＡＰ情報管理テーブル内に存在するか否かを検索し、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在しない場合には、前記ＡＰに対して公開鍵認証要求を行い、前記ＭＡＣアドレスが前記ＡＰ情報管理テーブル内に存在する場合には、前記ＡＰに対して公開鍵再認証要求を行うＳＴＡ（移動端末局）と、前記ＳＴＡからの前記公開鍵認証要求あるいは前記公開鍵再認証要求が妥当である場合には前記ＳＴＡの認証を行う前記ＡＰと、を備えることを特徴とする。

【００２５】また、前記ＡＰ情報管理テーブルは、前記ＳＴＡが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るＡＰのＭＡＣアドレスを最新認証完了実績順に保持することを特徴とする。

【００２６】さらに、前記ＡＰは、自らの秘密鍵であるＡＰ秘密鍵と、前記ＡＰ秘密鍵に対応する公開鍵であるところのＡＰ公開鍵と、前記ＡＰ公開鍵を付した自らのユーザ証明書であるところのＡＰユーザ証明書とを保持し、前記ＳＴＡは、自らの秘密鍵であるＳＴＡ秘密鍵と、前記ＳＴＡ秘密鍵に対応する公開鍵であるところのＳＴＡ公開鍵と、前記ＳＴＡ公開鍵を付した自らのユーザ証明書であるところのＳＴＡユーザ証明書とを保持している、ことを特徴とする。

【００２７】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して認証要求を行い、前記認証要求を受信した前記ＡＰから前記ＳＴＡに対して前記ＡＰユーザ証明書を送信し、前記ＡＰユーザ証明書を受信した前記ＳＴＡが、前記ＡＰユーザ証明書を検証した後に前記ＡＰユーザ証明書に添付された前記ＡＰ公開鍵を用いて前記ＳＴＡユーザ証明書を暗号化して暗号化ＳＴＡユーザ証明書を作成し、前記暗号化ＳＴＡユーザ証明書を前記ＡＰに対して送信し、前記暗号化ＳＴＡユーザ証明書を受信した前記ＡＰが、前記暗号化ＳＴＡユーザ証明書を前記ＡＰ秘密鍵で復号化して前記ＳＴＡユーザ証明書を再生し、前記ＳＴＡユーザ証明書を検証した後に前記ＳＴＡユーザ証明書に添付された前記ＳＴＡ公開鍵を用いて前記ＡＰが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化共通鍵を受信した前記ＳＴＡが、前記暗号化共通鍵を前記ＳＴＡ秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする。

【００２８】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」又は「１」でない任意の数「ｎ」である、ことを

特徴とする。

【００２９】また、前記ＡＰは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記ＡＰが過去に認証許可を通知した実績の有る前記ＳＴＡのＭＡＣアドレスと、該ＳＴＡの前記ＳＴＡ公開鍵と、前記ＡＰが該ＳＴＡの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする。

【００３０】さらに、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う場合には、前記ＳＴＡから前記ＡＰに対して再認証要求を行い、前記再認証要求を受信した前記ＡＰが、前記公開鍵再認証要求を送信した前記ＳＴＡのＭＡＣアドレスが前記ＡＰの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記ＳＴＡのＭＡＣアドレスが前記公開鍵管理テーブルに存在し、かつ、該ＭＡＣアドレスに対応する公開鍵であるところの前記ＳＴＡ公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記ＡＰは、当該ＳＴＡに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記ＳＴＡ公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記ＳＴＡに送信して認証許可を通知し、前記暗号化新共通鍵を受信した前記ＳＴＡが、前記暗号化新共通鍵を前記ＳＴＡ秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする。

【００３１】また、前記ＳＴＡが前記ＡＰに対して前記公開鍵再認証要求を行う際に送受信されるＭＡＣフレーム内のフレームボディ部のAlgorithm Numberの値は、「０」と「１」と「ｎ」でない任意の数「ｍ」である、ことを特徴とする。

【００３２】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００３３】図１は本発明の無線ＬＡＮシステムにおける認証装置の一実施形態を示すブロック図である。

【００３４】図１に示す本実施の形態は、無線ＬＡＮの基地局としてのＡＰ（Access Point：アクセスポイント）１と、ＡＰ１に帰属する移動端末局としての複数のＳＴＡ（Station ：ステーション）２（ＳＴＡ２－１、ＳＴＡ２－ｋ）とから構成されている。図１に示す実施の形態は、IEEE802.11で定義するところのInfrastructure（インフラストラクチャ）方式であり、このような無線ＬＡＮネットワークの最小単位をＢＳＳ（Basic Service Set ：基本サービス・セット）４と言う。

【００３５】ＢＳＳ４内におけるＡＰ１は、各ＳＴＡ２がＡＰ１に同期するための情報を含むBeacon（ビーコン）フレームを、周期的にＢＳＳ４内にブロードキャスト送信し、当該Beaconフレームを受信したＢＳＳ４内の各ＳＴＡ２は、通信開始時にＡＰ１に対して認証要求を行い、ＡＰ１により認証許可を受けた後、ＡＰ１への帰

属処理を完了することにより、ＡＰ１との通信を行うことが可能となる。また、Infrastructure方式におけるＢＳＳ４内の各ＳＴＡ２は、ＳＴＡ２間通信時においてもＡＰ１を介した通信を行う。

【００３６】また、図１におけるＡＰ１は（portal）となっているが、Portalとは、IEEE802.11以外のＬＡＮプロトコルとのプロトコル変換機能をＡＰ１に付加したことを示しており、基地局としてのＡＰ１とＥｔｈｅｒｎｅｔ（登録商標）（イーサネット（登録商標））５などの有線ＬＡＮとの接続を可能にした基地局であることを示している。

【００３７】なお、図１に示した実施の形態は、IEEE802.11に準拠したものであるが、本実施の形態においては無線区間の暗号化及び認証の方式として、Shared Key方式（共通鍵認証方式）とは異なり、主として秘密鍵と公開鍵を用いた認証方式を採用している。従って、Shared Key方式と区別するために、本実施形態における認証方式を公開鍵認証方式と便宜的に呼ぶこととする。

【００３８】次に、図２を参照して、ＡＰ１とＳＴＡ２の詳細構成について説明する。

【００３９】図２は、ＡＰとＳＴＡの一例を示す詳細ブロック図である。

【００４０】図２において、上段のブロック図がＡＰ１であり、下段のブロック図がＳＴＡ２である。

【００４１】ＡＰ１は、図２に示す無線ＬＡＮカード１９－１と上位レイヤとのインターフェースであるところの上位レイヤインターフェース１７－１を介して、ＴＣＰ／ＩＰ（Transport Control Protocol/Internet Protocol）や各種アプリケーションなどの上位プロトコル処理を、基地局端末本体１８にて実現するものであり、ＳＴＡ２は、図２に示す無線ＬＡＮカード１９－２と上位レイヤとのインターフェースであるところの上位レイヤインターフェース１７－２を介して、ＡＰ１と同様な上位プロトコル処理を、ノート型パーソナルコンピュータなどの移動端末本体２０によって実現するものである。

【００４２】図２に示す無線ＬＡＮカード１９－１と無線ＬＡＮカード１９－２は、同一の構成を備える。従って、無線ＬＡＮカード１９において同一の構成要素に対応するものは、同一の参照数字または符号を付しておくものとする。

【００４３】図２に示す無線ＬＡＮカード１９（１９－１及び１９－２）は、無線区間でのフレーム送受信を行う無線機部１２と、変復調処理を行うIEEE802.11 PHY（Physical Layer：物理層）プロトコル処理部１３と、ＭＡＣ（Medium Access Control ：媒体アクセス制御）層でのアクセス制御を行うIEEE802.11 MACプロトコル処理部１４と、ＭＡＣ層での認証処理などの上位レイヤ処理を、内蔵するＣＰＵとメモリ１６によって実現する上位レイヤ処理部１５と、上位レイヤ処理部１５が使用するメモリ１６とから構成されている。

【００４４】次に、図３を参照して、ＳＴＡ２がＡＰ１に対して認証を要求する際に、ＳＴＡ２とＡＰ１間で送受信されるＭＡＣフレームについて説明する。

【００４５】図３は、認証要求時にＡＰとＳＴＡ間で送受信されるＭＡＣフレームの構成を説明する図である。

【００４６】ＳＴＡ２のＡＰ１に対する認証要求時には、図３に示すIEEE802.11のＭＡＣフレームフォーマットに従うＭＡＣフレーム３０－１が、ＡＰ１とＳＴＡ２間で交換され、ＭＡＣフレーム３０－１は、MAC Header（ＭＡＣヘッダー）３０－２と、FrameBody （フレームボディ）３０－３とFCS （Frame Check Sequence：フレームチェックシーケンス）３０－４とから構成されている。

【００４７】そして、Infrastructure方式におけるMAC Header３０－２は、各種フレームタイプや制御情報を示すFrame Control （フレームコントロール）３０－１１のフィールドと、送信先がビジーである場合に送信待機を行うための時間を定義するDuration（デュレーション）３０－１２のフィールドと、フレーム送信先アドレスを示すDA（Destination Address ：送信先アドレス）３０－１３のフィールドと、フレームの送信元アドレスを示すSA（Source Address：送信元アドレス）３０－１４のフィールドと、ＢＳＳ４の識別情報を示すBSSID ３０－１５のフィールドと、フレーム送信順を示すSequence Control（シーケンスコントロール）３０－１６のフィールドから構成される。

【００４８】フレーム送信時、図２に示すIEEE802.11 MACプロトコル処理部１４では、上位レイヤ処理部１５からの送信要求フレームを、図３に示すFrameBody ３０－３に入れてカプセル化し、送信要求情報から作成したMAC Header３０－２をFrameBody ３０－３の前に付加し、当該MAC Header３０－２とFrameBody ３０－３に対するCRC32（Cyclic Redundancy Code 32bits）算出結果を、FCS ３０－４としてFrameBody ３０－３の後ろに付加することにより、図３に示すようなIEEE802.11 MACプロトコルに従うＭＡＣフレーム３０－１への変換を行う。続いて図２に示すIEEE802.11 PHYプロトコル処理部１３では、当該ＭＡＣフレーム３０－１に対する変調処理を行い、無線機部１２を経て当該ＭＡＣフレーム３０－１を空間上に送出することにより、送信処理が完了する。

【００４９】フレーム受信時、図２に示すIEEE802.11 MACプロトコル処理部１４では、無線機部１２を経てIEEE802.11 PHYプロトコル処理部１３にて復調処理を行った結果として受信したＭＡＣフレーム３０－１に対してCRC32 の計算を行い、受信フレーム内のFCS ３０－４の値とCRC32 算出結果とが一致する場合には、MAC Header３０－２の内容の解析と受信フレームに対する処理を行い、FrameBody ３０－３の部分を上位レイヤ処理部１５へ通知する。

【００５０】次に、図４及び図５を参照して、本実施形

態の重要な構成要素としての公開鍵管理テーブル及びＡＰ情報管理テーブルについて説明する。

【００５１】図４は、ＡＰが保持する公開鍵管理テーブルを説明する図であり、図５は、ＳＴＡが保持するＡＰ情報管理テーブルを説明する図である。

【００５２】ＡＰ１は、図４に示す公開鍵管理テーブル４０を、図２に示す無線ＬＡＮカード１９－１のメモリ１６内に保持している。公開鍵管理テーブル４０は、ＡＰ１が過去に本発明の公開鍵認証において認証許可を行った実績の有るＳＴＡ２のＭＡＣ層の物理アドレスであるところのＭＡＣアドレスを保持するSTA Mac Address（ＳＴＡのＭＡＣアドレス）４０－１の欄と、当該ＳＴＡ２の公開鍵を保持するPublic Key（パブリックキー）４０－２の欄と、ＡＰ１が認証許可時に当該ＳＴＡ２に対して発行した共通鍵を保持するShared Key（シェアードキー）４０－３の欄とから構成されている。そして、ＡＰ１は公開鍵管理テーブル４０の各行を、ＳＴＡ２の最新認証許可順に登録する。

【００５３】ＳＴＡ２は、図５に示すＡＰ情報管理テーブル５０を、図２に示す無線ＬＡＮカード１９－２のメモリ１６内に保持している。ＡＰ情報管理テーブル５０は、ＳＴＡ２が本発明の公開鍵認証を要求して該公開鍵認証の完了実績の有るＡＰ１のＭＡＣアドレスを保持するAP MAC Address（ＡＰのＭＡＣアドレス）５０－１の欄から構成されており、ＳＴＡ２はＡＰ情報管理テーブル５０の各行を、ＡＰ１の最新認証完了実績順に登録する。

【００５４】ＡＰ１は、図４にて説明した公開鍵管理テーブル４０への情報登録時には、登録済みのSTA MAC address ４０－１の検索を行い、既に登録済みの同一ＭＡＣアドレスが存在する場合には、登録内容の情報更新と共に公開鍵管理テーブル４０の先頭の行へ当該情報を移動する。また、本発明の公開鍵認証完了後のフレーム暗号化通信の実施毎に、ＡＰ１は公開鍵管理テーブル４０のSTA MAC address ４０－１の検索を行い、通信相手のＳＴＡ２の管理情報を公開鍵管理テーブル４０の先頭の行へ移動することにより、通信機会が新しい通信相手の管理情報ほど管理テーブル上位に位置付けることで、公開鍵管理テーブル４０が限界登録数に達し、新規情報登録が不可能となった場合には、公開鍵管理テーブル４０内で最も下位に位置する通信機会の最も古い通信相手の管理情報を削除することで対応する。

【００５５】また、ＳＴＡ２はＡＰ１と同様に、図５にて説明したＡＰ情報管理テーブル５０への情報登録時には、登録済みのAP MAC address５０－１の検索を行い、既に登録済みの同一ＭＡＣアドレスが存在する場合には、登録内容の情報更新と共にＡＰ情報管理テーブル５０の先頭の行へ当該情報を移動する。また、本発明の公開鍵認証完了後のフレーム暗号化通信の実施毎に、ＳＴＡ２はＡＰ情報管理テーブル５０のAP MAC address５０－１の検索を行い、通信相手のＡＰ１の管理情報をＡＰ情報管理テーブル５０の先頭の行へ移動することにより、通信機会が新しい通信相手の管理情報ほど管理テーブル上位に位置付けることで、ＡＰ情報管理テーブル５０が限界登録数に達し、新規情報登録が不可能となった場合には、ＡＰ情報管理テーブル５０内で最も下位に位置する通信機会の最も古い通信相手の管理情報を削除することで対応する。

【００５６】次に、図６、図７、図８、図９を参照して、本実施形態の動作について説明する。

【００５７】本実施形態においては、図１に示した無線ＬＡＮシステムの、基地局であるＡＰ１と移動端末局であるＳＴＡ２は、共に、自らの秘密鍵とそれに対応する公開鍵、及び該公開鍵を添付したユーザ証明書を保持しているものとする。そして、当該ユーザ証明書は、認証機関に代表される第三者によって、公開鍵とその保有者（すなわち、ＡＰ１或いはＳＴＡ２）との関係、及び保有者自身の正当性を証明可能である、という条件を前提とするものとする。以下では、ユーザ証明書はデジタルユーザ証明書を意味するものとする。

【００５８】図１におけるＳＴＡ２がＡＰ１を介しての無線通信を行おうとする場合には、ＳＴＡ２は先ずＡＰ１に対して、本発明の公開鍵認証要求を送信することから開始する。

【００５９】ＳＴＡ２は公開鍵認証開始時に、認証要求先のＡＰ１のＭＡＣアドレスを用いて図５に示したＡＰ情報管理テーブル５０内のAP MAC Address５０－１の検索を行い、ＡＰ情報管理テーブル５０内に認証要求先ＡＰ１のＭＡＣアドレスが存在しない場合には、初回の認証要求として図６に示す公開鍵認証手順を行い、認証要求先ＡＰ１のＭＡＣアドレスが存在する場合には、過去に当該ＡＰ１との公開鍵認証の完了実績が有る場合であるため、再認証として、図８に示す公開鍵再認証手順を行う。

【００６０】先ず、初回の認証要求としての公開鍵認証手順について、図６及び図７を参照して説明する。

【００６１】図６は、公開鍵認証手順を示す図であり、図７は、公開鍵認証手順において送受信されるＭＡＣフレームのフレームボディ部（図３のFrameBody３０－３）を示す図である。

【００６２】図６において、ＡＰ１に対して公開鍵認証手順による認証要求を行うＳＴＡ２は、ＡＰ１に対して認証フレーム６１を送信する（ステップＳ６１）。認証フレーム６１のフレームボディ部は、図７の（１）認証フレーム６１に示す形式となっており、Algorithm Number（アルゴリズム番号）７０－１－１を「ｎ」とし、Transaction Sequence Number （トランザクションシーケンス番号）７０－１－２を「１」としたフレームとなっている。なお、公開鍵認証手順における認証時には、Algorithm Number７０－１－１～７０－４－１は常に

15

「ｎ」（ｎは「０」又は「１」でない任意の数）であるものと定義する。Algorithm Number７０－１－１～７０－４－１を「ｎ」とすることにより、Shared Key方式による認証手順と区別することが可能となる。

【００６３】ステップＳ６１でＳＴＡ２から公開鍵認証要求を受信したＡＰ１は、認証フレーム６２を用いてＡＰ１の保持するユーザ証明書をＳＴＡ２に対して送信する（ステップＳ６２）。認証フレーム６２は、図７の（２）認証フレーム６２に示す形式となっており、Algorithm Number７０－２－１は前述の通り「ｎ」であり、Transaction Sequence Number ７０－２－２は「２」で、APのユーザ証明書７０－２－３にＡＰ１の保持するユーザ証明書（ユーザ証明書に付随するＡＰ１の公開鍵をも付したもの）を挿入したフレームとなっている。

【００６４】ステップＳ６２でＡＰ１から認証フレーム６２を受信したＳＴＡ２は、ＡＰ１から受信したＡＰ１のユーザ証明書の内容を検証して、ＡＰ１のユーザ証明書の検証結果に問題の無いことを確認すると、ＡＰ１のユーザ証明書に添付された公開鍵を用いて、ＳＴＡ２の保持するユーザ証明書の暗号化を行う（ステップＳ６３）。そして、暗号化したＳＴＡ２のユーザ証明書を、ＳＴＡ２のユーザ証明書に付随するＳＴＡ２の公開鍵と共に、認証フレーム６３を用いてＡＰ１に対して送信する（ステップＳ６４）。認証フレーム６３は、図７の（３）認証フレーム６３に示す形式となっており、Algorithm Number７０－３－１は前述の通り「ｎ」であり、Transaction Sequence Number ７０－３－２は「３」で、APの公開鍵で暗号化したSTA のユーザ証明書７０－３－３を付加したフレームとなっている。

【００６５】ステップＳ６４で認証フレーム６３を受信したＡＰ１は、APの公開鍵で暗号化したSTA のユーザ証明書７０－３－３をＡＰ１の秘密鍵で復号化して、ＳＴＡ２のユーザ証明書の内容を検証し、ＳＴＡ２のユーザ証明書の検証結果に問題の無いことを確認すると、次に今度は共通鍵を生成し、ＳＴＡ２のユーザ証明書に添付された公開鍵を用いて生成した共通鍵を暗号化する（ステップＳ６５）。そして暗号化した共通鍵を、認証フレーム６４を用いてＳＴＡ２に送信し、認証許可を通知する（ステップＳ６６）。認証フレーム６４は、図７の（４）認証フレーム６４に示す形式となっており、Algorithm Number７０－４－１は前述の通り「ｎ」であり、Transaction Sequence Number ７０－４－２は「４」で、STA の公開鍵で暗号化した共通鍵７０－４－３を付加したフレームとなっている。なお、図７に示したStatus Code ７０－１－９、Status Code ７０－２－９、Status Code ７０－３－９及びStatus Code ７０－４－９は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【００６６】その後、ステップＳ６６でＡＰ１から認証フレーム６４を受信したＳＴＡ２は、STA の公開鍵で暗号化した共通鍵７０－４－３をＳＴＡ２の秘密鍵で復号化して、ＡＰ１が生成した共通鍵を復元し、この後実際に行われる無線通信におけるフレーム暗号化に、該共通鍵を使用することとなる（ステップＳ６７）。以上の動作により、公開鍵認証手順が終了となり、以後、ＳＴＡ２とＡＰ１間でフレーム暗号化通信が行われることとなる。

【００６７】次に、再認証が行われる際の公開鍵再認証手順について、図８及び図９を参照して説明する。

【００６８】図８は、公開鍵再認証手順を示す図であり、図９は、公開鍵再認証手順において送受信されるＭＡＣフレームのフレームボディ部（図３のFrameBody３０－３）を示す図である。

【００６９】図８において、認証要求先のＡＰ１に対して過去に公開鍵認証完了実績のあるＳＴＡ２は、公開鍵再認証要求としてＡＰ１に対して認証フレーム８１を送信する（ステップＳ８１）。認証フレーム８１のフレームボディ部は、図９の（１）認証フレーム８１に示す形式となっており、Algorithm Number（アルゴリズム番号）９０－１－１を「ｍ」とし、Transaction Sequence Number （トランザクションシーケンス番号）９０－１－２を「１」としたフレームとなっている。なお、公開鍵再認証手順における認証時には、Algorithm Number９０－１－１～９０－２－１は常に「ｍ」（ｍは「０」と「１」と「ｎ」でない任意の数）であるものと定義する。Algorithm Number９０－１－１～９０－２－１を「ｍ」とすることにより、図６に示した公開鍵認証手順と区別することが可能となる。

【００７０】ステップＳ８１でＳＴＡ２から公開鍵再認証要求を受信したＡＰ１は、ＡＰ１が保持している図４に示した公開鍵管理テーブル４０において、公開鍵再認証要求を送信したＳＴＡ２のＭＡＣアドレスがSTA Mac Address ４０－１に存在するか検索を行う（ステップＳ８２）。そして、検索が成功し、かつ、それに対応する公開鍵をPublic Key４０－２の欄に保持していることを確認した場合には、ＡＰ１は当該ＳＴＡ２に対して指定する共通鍵を新たに生成し、この新共通鍵を公開鍵管理テーブル４０のPublic Key４０－２から取得した公開鍵（当該ＳＴＡ２の公開鍵）を用いて暗号化する（ステップＳ８３）。そして、暗号化した新共通鍵を、認証フレーム８２を用いてＳＴＡ２に送信する（ステップＳ８４）。認証フレーム８２は、図９の（２）認証フレーム８２に示す形式となっており、Algorithm Number９０－２－１は前述の通り「ｍ」であり、Transaction Sequence Number ９０－２－２は「２」で、STA の公開鍵で暗号化した新共通鍵９０－２－３を付加したフレームとなっている。なお、図９に示したStatus Code ９０－１－９及びStatus Code ９０－２－９は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。